UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO

MUTASEM JARDANEH, *et al.*

Plaintiffs,

v.

MERRICK GARLAND, in his official capacity as Attorney General of the United States,
et al.,

Defendants.

1:24 MC 0017

Misc. No. _____

Underlying Action: Case No. 8:18-cv-02415-PX (D. Md.)

MEMORANDUM OF LAW IN SUPPORT OF DEFENDANTS' MOTION TO QUASH AND EMERGENCY REQUEST FOR A STAY

INTRODUCTION

Under Rules 26(c)(1) and 45(d)(3) of the Federal Rules of Civil Procedure, the U.S. Government Defendants in the above-captioned action hereby move to quash two subpoenas ordering non-parties CommuteAir LLC and Mr. Erik Kane to appear for depositions and to produce documents in connection with ongoing litigation in the U.S. District Court for the District of Maryland, *see generally Jardaneh et al. v. Garland et al.*, Case No. 8:18-cv-02415-PX (D. Md.). Because both CommuteAir and Mr. Kane reside in this District, the Government brings the instant Motion to this Court pursuant to Fed. R. Civ. P. 45(d)(3)(a)(iii), which requires that "the court for the district where compliance is required must quash or modify a subpoena that . . . requires disclosure of privileged or other protected matter."

The Government also seeks an emergency stay of the depositions—currently scheduled for March 7, 2024—while the parties brief the instant Motion, or, in the alternative, a protective order that requires Plaintiffs[1] to withdraw the subpoenas pending motions practice, or pending a narrowing of the subpoenas that would address the weighty issues identified herein regarding disclosure of protected information. The Government has met and conferred with Plaintiffs' counsel, sought to narrow the issues subject to dispute, and proposed a briefing schedule on the instant Motion to Quash, but Plaintiffs declined to engage in a schedule without a court order, and declined to explain any need for the requested depositions to go forward at this juncture, when discovery is ongoing in the District of Maryland and Defendants agreed to stipulate to an extension of any necessary deadlines. *See* Exhibit 5.

[1] Throughout this filing, "Plaintiffs" refers to the plaintiffs in the underlying *Jardaneh* action in the District of Maryland, and "the Government" or "Defendants" refers to the official-capacity government defendants in that same action.

The subpoenas at issue here are directed to an airline (CommuteAir) that was the subject of an alleged data breach in January of 2023, as well as to a communications professional, Mr. Erik Kane, then an employee of the airline who gave certain statements to the media in the aftermath of the alleged breach. Through the subpoenas to CommuteAir and Mr. Kane, Plaintiffs seek to authenticate purportedly stolen government documents, where the underlying information—an alleged copy of the 2019 No-Fly List—is protected by the law enforcement privilege and is statutorily protected as Sensitive Security Information (SSI) pursuant to 49 U.S.C. § 114(r). *See* Declaration of Steve McQueen (attached as Exhibit 3); TSA Final SSI Order (attached as Exhibit 4).[2] Plaintiffs in the underlying litigation lost a Motion to Compel seeking discovery of their purported status on or off government watchlists (known as the Terrorist Screening Dataset or TSDS, of which the No Fly List is a subset): a federal magistrate judge determined that the information was shielded by the law enforcement privilege. *See* Exhibit 6. Other courts, including a session of this court, have recognized that "the TSD[S] status of a particular individual can neither be confirmed nor denied." *Shearson v. Holder*, 865 F. Supp. 2d 850, 861 n.2 (N.D. Ohio 2011), *aff'd*, 725 F.3d 588 (6th Cir. 2013); *see also Elhady v. Kable*, 993 F.3d 208, 215 (4th Cir. 2021) ("Disclosure would disrupt and potentially destroy counterterrorism investigations because terrorists could alter their behavior, avoid detection, and destroy evidence"). As detailed in this Motion, having already lost on this issue in ordinary party discovery—and with courts uniformly recognizing that TSDS status is not discoverable in civil litigation—it strains credulity to think that Plaintiffs, though not entitled to discovery of their own purported status on the TSDS, should be able to confirm or deny the authenticity of the *entire*

[2] This brief does not confirm or deny the authenticity of the allegedly stolen data. Any statements about the allegedly stolen data are not based on assumptions that it either is, or is not, authentic.

TSDS through the guise of a third-party subpoena directed at an airline that was itself under legal and contractual obligations to protect SSI. And there is no other plausible reason for Plaintiffs to seek this discovery, as the underlying litigation has nothing to do with CommuteAir or with the public relations and communications operations of any airline.

Plaintiffs should not be able to circumvent the rulings of the District Court in Maryland by subpoenaing a third party. Moreover, even on their own terms, the documents requested and the deposition topics listed on the subpoenas seek information that is protected by the law enforcement privilege and is statutorily protected as SSI, as explained by the attached McQueen Declaration and TSA Final Order. The Court should quash the subpoenas or, at minimum, grant a temporary stay of the underlying depositions to allow for further consideration and briefing on these issues.

PRELIMINARY REQUEST FOR A STAY

The third-party depositions in this case are currently scheduled for March 7, 2024. Defendants asserted their privilege and SSI objections to the subpoenas via written letter to Plaintiffs, and then have met and conferred with counsel for Plaintiffs and proposed a postponement of the currently-scheduled depositions and a briefing schedule on the Government's Motion to Quash. In exchange, the Government agreed not to object to the depositions continuing at a later date should Plaintiffs prevail, notwithstanding any upcoming fact discovery deadlines in the underlying litigation. *See* Exhibit 5. However, Plaintiffs declined to engage with the Government on a briefing schedule for this Motion. *Id.*

Given that the depositions are scheduled for March 7, 2024, the Government seeks an emergency stay of these depositions (and the corresponding request for document productions) pending the outcome of this miscellaneous action and Motion to Quash. There is no harm to the Plaintiffs in staying the depositions, as the depositions could go forth at a later date if the Plaintiffs

are successful in overcoming the Government's assertion of the law enforcement privilege. By contrast, as detailed further *infra*, the consequences for the Government and its law enforcement and counterterrorism operations to the depositions continuing as scheduled could be significant.

BACKGROUND

I. The Government's Watchlisting System

Several different components of the Federal Government work together to secure the United States and its borders and aviation system from terrorist threats. Within the Department of Homeland Security ("DHS"), TSA is responsible for securing all modes of transportation, with a focus on preventing terrorist attacks against civil aviation and other methods of transportation. *See* 49 U.S.C. § 114(d). TSA is further responsible for day-to-day federal security screening operations for passenger air transportation, 49 U.S.C. § 114(e)(l), and for developing "policies, strategies, and plans for dealing with threats to transportation security," *id.* § 114(f)(3). TSA may "issue . . . such regulations as are necessary to carry out [its] functions," *id.* § 114(l)(1), as well as "prescribe regulations to protect passengers and property on an aircraft," *id.* § 44903(b). The FBI investigates and analyzes intelligence relating to both domestic and international terrorist activities. *See* 28 U.S.C. § 533; 28 C.F.R. § 0.85(1). The FBI also administers the Terrorist Screening Center ("TSC"), a multi-agency Executive organization established by Presidential Directive in 2003 and tasked with, *inter alia*, "consolidat[ing] the Government's approach to terrorism screening and provid[ing] for the appropriate and lawful use of Terrorist Information in screening processes." Homeland Security Presidential Directive ("HSPD") 6 (Sept. 16, 2003) [https://perma.cc/BFP2-MBWQ].

As part of its duties, TSC maintains the Terrorist Screening Dataset ("TSDS"),[3] which is "the federal government's consolidated watchlist of known or suspected terrorists." *Elhady*, 993 F.3d at 213; *see also Mokdad v. Lynch*, 804 F.3d 807, 809 (6th Cir. 2015) (noting that the TSDS "is developed and maintained by the Terrorist Screening Center (TSC), a multi-agency center that was created in 2003 and is administered by the Federal Bureau of Investigation (FBI), which in turn is part of the Department of Justice"). Inclusion in the TSDS results from a multi-step assessment, based on analysis of available intelligence and investigative information about an individual. *See* Exhibit 7, "Overview of the U.S. Government's Watchlisting Process and Procedures as of September 2020" ("Watchlisting Overview"), at 3. The FBI receives, reviews, and forwards to the TSC "nominations" of individuals with a nexus to domestic terrorism for inclusion in the TSDS. *Id.* The National Counterterrorism Center, a component of the Office of the Director of National Intelligence, does the same for nominations of individuals with a nexus to international terrorism. *Id.* TSC then determines whether those nominations will be accepted. *Id.* For a nomination to be accepted, it must include enough identifying information to allow screeners to determine whether the individual matches a record in the TSDS, and enough information to satisfy a reasonable suspicion that the individual is a known or suspected terrorist. *Id.* The TSDS contains subsets of data, known as the No Fly List, the Selectee List, and the Expanded Selectee List. Inclusion on any of these lists requires satisfaction of additional criteria

[3] Until recently, the TSDS was known as the Terrorist Screening Database or the "TSDB," and the terms are used interchangeably in this memorandum, the accompanying exhibit, and case law.

distinct from, and over and above, that required for designation as a known or suspected terrorist and inclusion in the TSDS generally. *Id.*

One of the primary uses of the TSDS and its subsets is to ensure aviation security. For example, TSA uses TSDS information to "identify [travelers] who may be a threat to civil aviation or national security," 49 U.S.C. § 114(h)(3)(A), and to "prevent [those] individual[s] from boarding an aircraft, or take other appropriate action with respect to that individual," *id.* § 114(h)(3)(B); *id.* § 114(h)(1). The federal government also utilizes TSDS information for other purposes, including assisting state, local, and tribal governments with law enforcement and corrections.

Consistent with statutory and law enforcement privileges, as reflected in the McQueen Declaration, "it is the policy of the US Government not to disclose any individual's status in the TSDS or a subset, beyond the limited disclosures contemplated by [redress] procedures for US Persons who are denied boarding because of their presence on the No Fly List." Ex. 3, McQueen Decl. ¶ 20; *see also id.* ¶ 24 ("If the Government were required to reveal TSDS status outside of the above-described narrow exception, terrorists would be better able to circumvent counterterrorism efforts. For example, disclosure that an individual has a TSDS status that TSA relies upon to require enhanced security screening would arm terrorists with the knowledge of who would be required to undergo additional screening and who would not.").

Moreover, such status is protected by the law enforcement privilege, and the identities of those on the No Fly, Selectee, and Expanded Selectee lists are also statutorily protected as Sensitive Security Information ("SSI") pursuant to 49 U.S.C. § 114(r). *See, e.g., Blitz v. Napolitano*, 700 F.3d 733, 737 n.5 (4th Cir. 2012); *Scherfen v. U.S. DHS*, No. 3:CV-08-1554, 2010 WL 456784, at *8 n.5 (M.D. Pa. Feb. 2, 2010) ("Because the TSDB status of Plaintiffs can neither

be confirmed nor denied, this Court cannot discuss . . . the contents of [documents revealing Plaintiffs' status] submitted for *in camera* review[.]"); *see also* 49 C.F.R. § 1520.5(b)(9)(ii) (SSI includes "[i]nformation and sources of information used by a passenger or property screening program or system, including an automated screening system"); *see also* Protection of Sensitive Security Information, 69 Fed. Reg. 28066-01, 28071 (May 18, 2004) (interim final rule adding 49 C.F.R. § 1520.5(b)(9)(ii)) ("This is intended to cover . . . lists of individuals identified as threats to transportation or national security.")

As numerous courts have recognized, this nondisclosure serves to protect against significant national security harms. *See Elhady*, 993 F.3d at 215 ("Disclosure would disrupt and potentially destroy counterterrorism investigations because terrorists could alter their behavior, avoid detection, and destroy evidence"); *see also Shearson v. Holder*, 865 F. Supp. 2d 850, 861 n.2 (N.D. Ohio 2011) (recognizing that "the TSD[S] status of a particular individual can neither be confirmed nor denied"), *aff'd*, 725 F.3d 588 (6th Cir. 2013); *Beydoun v. Sessions*, 871 F.3d 459, 463 (6th Cir. 2017) ("the government has neither confirmed nor denied that Plaintiffs are on the Selectee List"); *Kalu v. IRS*, 159 F. Supp. 3d 16, 23 (D.D.C. 2016) ("[A]mong other adverse consequences of full or even partial disclosure [of TSDS status] is that '[r]equiring the government to reveal whether a particular person is on the watch lists would enable criminal organizations to circumvent the [TSDS's] purpose[.]'" (quoting *Gordon v. FBI*, 388 F. Supp. 2d 1028, 1037 (N.D. Cal. 2005)).[4]

[4] *Rhodes v. FBI*, 316 F. Supp. 3d 173, 178 (D.D.C. 2018) (similar); *Morgan v. FBI*, No. A-15-CA-1255-SS, 2016 WL 7443397, at *4 (W.D. Tex. May 24, 2016) (similar); *Wright v. FBI*, No. 3:20-CV-173-G-BN, 2020 WL 7345678, at *8 (N.D. Tex. Nov. 13, 2020) (similar); *Platsky v. Nat'l Sec. Agency*, No. 11-cv-4816-SLTRLM, 2013 WL 12121950, at *4 (E.D.N.Y. Jan. 30, 2013) (similar), *aff'd*, 547 F. App'x 81 (2d Cir. 2013); *Skurow v. DHS*, 892 F. Supp. 2d 319, 332 (D.D.C. 2012) (similar); *Tooley v. Bush*, No. 06-306, 2006 WL 3783142, at *20 (D.D.C. Dec. 21, 2006) (similar), *aff'd sub nom., Tooley v. Napolitano*, 586 F.3d 1006 (D.C. Cir. 2009); *Al-Kidd v.*

II. This Litigation and Plaintiffs' Efforts Seek Discovery Regarding Watchlist Status

The underlying lawsuit in this case was commenced in 2018 in the U.S. District Court for the District of Maryland, and the operative pleading was filed on March 22, 2019, *see* Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 48. The Complaint brings a variety of constitutional claims against various government defendants, all arising out of various individual plaintiffs' alleged placement on the TSDS. The parties are currently engaged in fact discovery, including a number of depositions that are ongoing.

Most relevant to the instant Motion, there has been substantial motions practice before the District of Maryland relating to TSDS/watchlist status. Plaintiffs filed a Motion to Compel that information on March 19, 2021, including to compel production of a privilege log. *See* Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 114. Defendants opposed, arguing that the information requested was protected by the law enforcement privilege.[5] On May 19, 2023, Judge Simms orally denied the Plaintiffs' motion to compel TSDS/watchlist status information. *See* Ex. 6. In particular, the court concluded that "I am wholly satisfied that disclosure of this information could be expected to risk circumvention of the law, of law enforcement efforts, and harm the United States' national security and counterterrorism efforts," and further held that "Disclosing this current or historical Watchlist status would reveal sensitive, closely guarded information about the internal workings of the watchlisting process, which I find could harm the United States's national

---

Gonzales, No. 05-093, 2007 WL 4391029, at *9 (D. Idaho Dec. 10, 2007) ("the public interest in [protecting information in the TSDS] weighs decidedly in favor of nondisclosure for security reasons."); *Raz v. Mueller*, 389 F. Supp. 2d 1057, 1062 (W.D. Ark. 2005) (similar). *Cf. Vazquez v. DOJ*, 887 F. Supp. 2d 114, 117-18 (D.D.C. 2012) (same, as to other FBI databases).

[5] TSA also issued an SSI Final Order in response to this Motion to Compel, which is attached to the SSI Order issued with respect to these subpoenas in Exhibit 4 at 8. Plaintiffs neglected to file a Petition for Review in a U.S. Court of Appeals challenging TSA's SSI designations in that case, as required under 49 U.S.C. § 46110.

security and counterterrorism mission." *Id.* at 24. The court later memorialized this ruling in a written order, finding that the Plaintiffs' discovery requests (as relevant here) "clearly seek Watchlist-related information from the Merits Defendants," which includes "information that confirms/denies—or is related to—the Watchlist status of any or all of the remaining Plaintiffs." *See* Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 227 at 1 & n. 1 (May 26, 2023).

III. The Current Subpoenas

On January 30, 2024, Plaintiffs' counsel sent an email to Defendants' counsel attaching copies of subpoenas purportedly served on CommuteAir and Mr. Erik Kane. *See* Exhibits 1 & 2. Service, however, was never properly made, or if it was, proof of such service was never communicated to the Government. The Certificates of Service on both subpoenas (from the District of Maryland) were blank, suggesting that they had never been filled out or properly issued. Additionally, the Certificates of Service on the Deposition Notices were purportedly signed by Amy Powell, but Ms. Powell is an attorney for the Department of Justice and in fact is counsel for *Defendants* in the underlying action, not the *Plaintiffs*, and so would not be issuing subpoenas seeking law enforcement privileged information from third parties.

In any event, counsel for CommuteAir, Peter Turner, served objections to the subpoena served on CommuteAir on February 2, 2024. *See* Ex. 8. The CommuteAir deposition was then scheduled for March 7, 2024. *See* Ex. 9. Although counsel for the Government was unable to confirm whether service had been properly made, the Government served written objections on February 16, 2024. *See* Ex. 10. In that letter, the Government explained that "the documents requested, and the deposition topics listed on the subpoena, appear to be an effort to authenticate or corroborate an alleged data breach, for the apparent purpose of expert discovery. However, information confirming or denying the authenticity of the allegedly stolen data is protected by the

law enforcement privilege, and is statutorily protected as Sensitive Security Information ("SSI") pursuant to 49 U.S.C. § 114(r). Therefore, the subpoenas in their current form are improper." *Id.*

Counsel for the Government also proposed that the deposition topics could be narrowed to ameliorate the Government's concerns. Namely, "if the deposition were limited to non-SSI and non-Law Enforcement Sensitive information on the first topic in Exhibit A ("The process by which official comments by CommuteAir officials release statements to the press or the public"), without any discussion of the No Fly List, Selectee List, or any other government watchlist, and without any questions or discussion of the alleged incident referenced in Exhibit A, Item 3 (statement to the Daily Dot regarding the alleged data incident), Defendants could perhaps agree to such a narrowing." *Id.* Similarly, counsel wrote, "if the list of documents in Exhibit B were limited to non-SSI and non-Law Enforcement Sensitive documents responsive to Item 1, and excluded items 2-7, Defendants would be agreeable to such documents being produced without seeking relief from the court."[6]

Finally, the Government proposed a meet-and-confer to discuss a possible schedule on briefing for motions practice if the parties were unable to agree to narrow the deposition topics, and also offered to agree that, if the Government were to lose its forthcoming Motion to Quash, the Government would not object to the depositions going forward based on any upcoming fact discovery cut-off dates in the District of Maryland litigation. *See id.* The parties conferred by phone on February 20, 2024. In that call, Plaintiffs' counsel asked for a proposed schedule, but did not indicate whether Plaintiffs would agree to pause the depositions then scheduled for March

[6] In the February 16, 2024 Objection Letter, the Government noted that it was unaware whether service had been made on Mr. Kane, but "reserve[d] all objections regarding the scope of that deposition and request for documents, to the extent that they go forward." *See* Ex. 10. That same day, counsel for CommuteAir indicated that service had been made on Mr. Kane, and his deposition has now been scheduled for the same day—March 7, 2024. *See* Exhibit 11.

7, 2024. Government counsel followed up with a proposed briefing schedule on February 22, under which briefing would be completed by March 22, and reiterated that the Government would agree that the depositions could go forward notwithstanding any other case deadlines should Plaintiffs prevail. Plaintiffs declined. *See* Exhibit 5.

Separately, the Government understands that counsel for CommuteAir would plan to produce certain documents responsive to the subpoenas on March 4, with the depositions occurring over Zoom on March 7. Defendants therefore seek, at a minimum, an emergency stay of the current deposition dates and corresponding schedule for document production to address the privilege issues detailed in this memorandum.

LEGAL STANDARD

Federal Rule of Civil Procedure 45 governs subpoenas issued to non-parties. *See* Fed. R. Civ. P. 45. Under Rule 45, the Court "must quash or modify a subpoena that . . . subjects a person to undue burden," or that "requires disclosure of privileged or other protected matter, if no exception or waiver applies." Fed. R. Civ. P. 45(d)(3)(A). *See United States v. Tenn. Walking Horse Breeders' and Exhibitors Ass'n*, 727 Fed. Appx 119, 123 (6th Cir. 2018) ("A court must protect a non-party subject to a subpoena if it 'requires disclosure of privileged or other protected matter'" (quoting Fed. R. Civ. P. 45(d)(3)(A)(iii-iv)). Because the scope of discovery under Rule 45 tracks Rule 26, standards for discovery under both rules govern a motion to quash. *See Gard v. Grand River Rubber & Plastics Co.*, No. 1:20CV125, 2021 WL 75655, at *4–5 (N.D. Ohio Jan. 8, 2021). Rule 26 grants broad discretion to make any order which justice requires "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense," including to forbid the proposed discovery altogether. Fed. R. Civ. P. 26(c)(1); *see also Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 36 (1984). Under Rule 26(b)(2), in particular, the court

"must limit the frequency or extent of discovery . . . if it determines that . . . the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive." Fed. R. Civ. P. 26(b)(2)(C). Rule 45, however, expands on Rule 26 by also taking into account the interest of non-parties. *See Watts v. SEC*, 482 F.3d 501, 509 (D.C. Cir. 2007) (opinion for the Court by Kavanaugh, J.) (Rule 45 "requires district courts supervising discovery to be generally sensitive to the costs imposed on third parties").

The Sixth Circuit has also recognized an exception to the usual rule that "a party has no standing to seek to quash a subpoena issued to someone who is not a party to the action" where "the party claims some personal right or privilege with regard to the documents sought." *Mann v. University of Cincinnati*, 114 F.3d 1188 (Table), 1997 WL 280188, at *4 (6th Cir. May 27, 1997) (quoting 9A Charles Alan Wright and Arthur R. Miller, Federal Practice and Procedure § 2459 (1995)). *Cf. Donahoo v. Ohio Dept. Of Youth Services*, 211 F.R.D. 303, 306 (N.D. Ohio 2002) ("*absent a claim of privilege*, a party has no standing to challenge a subpoena to a nonparty.") (emphasis added"); *see also Malibu Media, LLC v. Doe*, No. 1:14-CV-02744, 2015 WL 1291458, at *2 (N.D. Ohio Mar. 23, 2015) (finding standing to quash subpoena where there was "some personal right or privilege" in the information sought). The party seeking to quash a subpoena "bears the burden of establishing that the issued subpoenas violate Rule 45 of the Federal Rules of Civil Procedure." *Recycled Paper Greetings, Inc. v. Davis*, No. 1:08-MC-13, 2008 WL 440458, at *3 (N.D. Ohio Feb. 13, 2008). "If the documents sought by the subpoena are 'relevant and are sought for good cause,' then the subpoena should be enforced 'unless the documents are privileged or the subpoenas are unreasonable, oppressive, annoying, or embarrassing.'" *Chao v. Local 951, United Food and Commercial Workers International Union*, 2006 WL 2380609, at *2 (N.D. Ohio 2006) (citing *Bariteau v. Krane*, 206 F.R.D. 129, 130 (W.D. Ky. 2001)).

It is well established that "[t]rial courts have broad discretion and inherent power to stay discovery until preliminary questions that may dispose of the case are determined." *Hahn v. Star Bank*, 190 F.3d 708, 719 (6th Cir. 1999); *see also Gray v. Bush*, 628 F.3d 779, 785 (6th Cir. 2010) (district courts have inherent power "to stay proceedings" to "control the disposition of the causes on its docket with economy of time and effort for itself, for counsel, and for litigants."). A party requesting a stay of discovery production must show: "(1) whether the stay applicant has made a strong showing that he is likely to succeed on the merits; (2) whether the applicant will be irreparably injured absent a stay; (3) whether the issuance of the stay will substantially injure the other parties interested in the proceeding; [and] (4) where the public interest lies." *Hilton v. Braunskill*, 481 U.S. 770, 776 (1987)); *see also J & R Passmore, LLC v. Rice Drilling D, LLC*, No. 2:18-CV-01587, 2023 WL 2633671, at *3 (S.D. Ohio Mar. 24, 2023) ("A party requesting a stay of discovery production must" satisfy the *Braunskill* factors); *Adkisson v. Jacobs Eng'g Grp., Inc.*, No. 3:13-CV-505-TAV-HBG, 2020 WL 8255191, at *1 (E.D. Tenn. Nov. 10, 2020) ("When a party seeks a stay of discovery, the Court 'weighs the burden of proceeding with discovery upon the party from whom discovery is sought against the hardship which would be worked by a denial of the discovery.'") (citation omitted).

ARGUMENT

I. The Subpoenas Represent an Improper End-Run Around Party Discovery and Contradict a Ruling on a Prior Motion to Compel by a Federal Magistrate Judge.

As an initial matter, the primary underlying issue—whether Plaintiffs should gain access to the TSDS against the Government's claim of privilege—has already been resolved in the Government's favor in the underlying litigation. Plaintiffs' effort to take another bite at the apple in another court through the stratagem of seeking to have a third party confirm or deny the

authenticity of an allegedly stolen document purporting to include that privileged information should be likewise rejected.

Specifically, through interrogatories, Plaintiffs sought particular individuals' current and historical status in the TSDS, and then filed a Motion to Compel when the Government refused to produce that information and declined to produce a privilege log. Plaintiffs objected, noting that "[a]ccording to the Government, even confirming that they are withholding information would let Plaintiffs know that they are on the federal terrorism watchlist, which is supposedly privileged." *See* Plaintiffs' Motion to Compel, Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 114 at 8 (March 19, 2021). Similarly, Plaintiffs argued that "Plaintiff's [sic] watchlist placement is not formally classified. At most, it is protected as SSI, a relatively basic form of protected information and one Plaintiffs' counsel should have access for." *See* Plaintiff's Reply Brief in Support of Motion to Compel, Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 135 at 11 (May 24, 2021).

The District Court disagreed and held that Plaintiffs' TSDS status was, in fact, protected by the law enforcement privilege. Initially, in a written ruling, the Court noted that the "redacted declarations provide sufficient detail for the Court to find that the law enforcement privilege applies to the four categories of withheld documents," *see* Memorandum Opinion, Case No. 8:18-cv-02415-PX (D. Md.), ECF 162 at 19 (Sept. 14, 2021), and the Court in turn "reserve[d] ruling on whether Plaintiffs have established a compelling need for the plaintiff-specific documents, and whether their need outweighs the Defendants' legitimate law enforcement interests." *Id.* at 21. However, at a subsequent oral ruling, the Court rejected Plaintiffs' arguments and categorically held that TSDS status was not discoverable. *See* Exhibit 6 at 24 ("I am wholly satisfied that disclosure of this information could be expected to risk circumvention of the law, of law enforcement efforts, and harm the United States' national security and counterterrorism efforts.

Disclosing this current or historical Watchlist status would reveal sensitive, closely guarded information about the internal workings of the watchlisting process, which I find could harm the United States's national security and counterterrorism mission."). The court later memorialized this ruling in a written order, finding that the Plaintiffs' discovery requests (as relevant here) "clearly seek Watchlist-related information from the Merits Defendants," which includes "information that confirms/denies—or is related to—the Watchlist status of any or all of the remaining Plaintiffs." *See* Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 227 at 1 & n.1 (May 26, 2023).

The District Court in Maryland, in other words, prevented Plaintiffs from getting access through discovery to the TSDS status of the individual Plaintiffs in the lawsuit, so it would be violative of the spirit of that Court's order if Plaintiffs could nonetheless be allowed to attempt to confirm the authenticity (or lack thereof) of what purports to be hundreds of thousands of names from a subset of the TSDS through the simple expedient of subpoenaing a third party that was the subject of an alleged data breach.

Nor is this the only time that Plaintiffs have sought to use allegedly leaked materials in discovery against Defendants. For example, in a March 23, 2023, Motion to Compel, Plaintiffs sought additional discovery regarding what the Government knew about the religious affiliations of particular individuals on the TSDS, arguing in support that "after studying more than 1.5 million leaked watchlist entries, Plaintiffs' statistical expert estimates with 95% certainty that 98.3% of watchlist entries identify Muslim names." *See* Plaintiffs' March 23, 2023, Motion to Compel, Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 230-2, at 30. Plaintiffs' Motion, in turn, claimed to attach the very purportedly stolen documents that are the subject of the alleged data incident here. *See id.* at 30; *see also* Case No. 8:18-cv-02415-PX (D. Md.), ECF No. 230-8 at 34 (Defendants'

Opposition) (noting that Plaintiffs were relying on "a purported statistical expert report which does not comply with the disclosure requirements of Rule 26(a)(2)(B), and which is based on an allegedly leaked copy of certain purported information from the TSDS."). In that same Motion to Compel, Plaintiffs sought to "authenticate a purportedly leaked copy of the 2013 [Watchlisting Guidance]," *id.* at 15, and the Government explained that confirming or denying the authenticity of the Guidance was protected by the law enforcement privilege and SSI. As the Government explained, any release or authentication would "provide terrorists and their associates with a roadmap of the specific techniques and procedures" that the Government uses to protect against terrorism. *See id.* at 16. That Motion to Compel remains pending before the Magistrate Judge, but it is telling that Plaintiffs continue to rely on purportedly leaked documents and appear to pay no mind to the Magistrate Judge's rulings upholding the Government's assertions of law enforcement privilege over TSDS information, of which these subpoenas are simply the most recent example.

II. The Subpoenas Seek Information That is Protected by the Law Enforcement Privilege and is Statutorily Protected as Sensitive Security Information (SSI).

Setting aside the improper effort to circumvent a ruling by the district court that is supervising discovery in this case, even on their own terms the subpoenas seek information that is 1) protected by the law enforcement privilege, and 2) constitutes Sensitive Security Information (SSI) pursuant to a Final Order from TSA. The subpoenas therefore present the same law enforcement concerns that animated the U.S. District Court for the District of Maryland's previous ruling denying Plaintiffs' Motion to Compel TSDS status information, and, as explained below, the result is unchanged even though the subpoenas are directed at third parties using the cloak of questions about previous public statements made to the media. Moreover, should Plaintiffs wish to challenge the SSI Final Order issued by TSA, they would need to pursue a Petition for Review

in an appropriate U.S. Court of Appeals, which holds exclusive jurisdiction to review TSA's SSI designations pursuant to 49 U.S.C. § 46110.

A. The Subpoenas Seek Information That is Protected by the Law Enforcement Privilege.

The purpose of the law enforcement privilege "is to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." *Noakes v. Case W. Rsrv. Univ.*, No. 1:21-CV-01776-PAB, 2022 WL 17811630, at *5 (N.D. Ohio Dec. 19, 2022) (quoting *In re Dep't of Investigation of City of New York*, 856 F.2d 481, 484 (2d Cir. 1988)). Once properly asserted by an official with knowledge of the information, there is a strong presumption against lifting the privilege, and to rebut the presumption, the party seeking disclosure must show (1) that its suit is non-frivolous and brought in good faith, (2) that the information sought is not available through other discovery or from other sources, and (3) a compelling need for the information. *See In re The City of New York*, 607 F.3d 923, 945 (2d Cir. 2010); *see also Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1125 (7th Cir. 1997) (explaining that "there ought to be a pretty strong presumption against lifting the privilege," given that "the United States places the control of such investigations firmly in the executive branch"). Even "demonstrating a 'compelling need' does not automatically entitle a litigant to privileged information. Rather, disclosure is required only if that compelling need outweighs the public interest in nondisclosure." *In re The City of New York*, 607 F.3d at 945.

Here, Defendants assert the law enforcement privilege via the Declaration of Steven McQueen, the Deputy Director of the Terrorist Screening Center.[7] As Mr. McQueen explains, "authentication of the subject documents could reasonably be expected to risk circumvention of the law and cause harm to national security." McQueen Decl. ¶ 34. Specifically, "[d]isclosure of such TSDB status would also allow known or suspected terrorists to more effectively and intelligently plan and carry out a domestic or international attack," and "[i]mportantly, individuals who are selected for enhanced security screening, unlike individuals who are denied boarding, are able to access sterile areas of airports and fly via commercial aviation, which remains a prime target for terrorist groups and individuals intending to perform attacks. Armed with knowledge of TSDB status, the individual (and/or his associates, or other interested parties) may rely on social engineering to abbreviate or distract screeners from the screening process." *Id.* ¶ 26. Many courts have upheld this important non-disclosure policy. *See, e.g., Elhady*, 993 F.3d at 215 ("[T]he government has a general policy of not disclosing TSDB status, whether positive or negative, in response to inquiries. The reason for this is apparent . . . Disclosure would disrupt and potentially destroy counterterrorism investigations because terrorists could alter their behavior, avoid detection, and destroy evidence").

Nor does it make any difference here that the subpoena is directed at a third party, or that it nominally seeks to ask the third-party questions about its statements to the media. As the McQueen Declaration explains: "The information requested from CommuteAir and Mr. Kane in the subpoenas issued by Plaintiffs would tend to reveal Law Enforcement privileged information

[7] The McQueen Declaration contains certain information that is marked Law Enforcement Sensitive and thus cannot be lodged on the public docket. A redacted version of that declaration accompanies this Motion as Exhibit 3. The Government will separately submit the unredacted declaration for the Court's *in camera, ex parte* review.

insofar as Plaintiffs seek to ask these third-parties to opine on the authenticity of the allegedly stolen government documents or to produce documents that may or may not suggest the underlying information is authentic. These subpoenas, therefore, risk of circumvention of the law and could cause reasonably be expected to harm to national security." *Id.* ¶ 32. Indeed, while the third party is the target of the subpoenas, if the underlying data is authentic—which this brief neither confirms nor denies—it would be protected by SSI and law enforcement privileged information, and airlines are under obligations to protect SSI and law enforcement privileged information as a condition of any agreement to access the information.

Plaintiffs cannot rebut the presumption of law enforcement privilege because, even assuming they could show a compelling need for the information, "disclosure is required only if that compelling need outweighs the public interest in nondisclosure." *In re The City of New York,* 607 F.3d at 945. As the District Court for the District of Maryland determined, the Government's declarations made "abundantly clear that release of the law enforcement sensitive information to Plaintiffs and/or their counsel, even subject to a protective order, reasonably could be expected to risk circumvention of the law and harm national security," and that "the Plaintiffs' compelling need for disclosure does not outweigh the public interest in nondisclosure. The public interest in nondisclosure is stronger here than the needs of Plaintiffs to have access to the privileged information." *See* Ex. 6 at 23-25. The same result obtains here, where Plaintiffs are trying to achieve the same result through the guise of third-party discovery.

B. The Subpoenas Seek Information that Statutorily Protected as Sensitive Security Information (SSI).

In addition to seeking information that is shielded from disclosure by the Law Enforcement Privilege, TSA has issued a Final Order determining that the subpoenas seek information that is statutorily protected as SSI because "[a]dmitting or denying the authenticity of the allegedly leaked

data would tend to confirm or deny whether the alleged data breach resulted in the hacker obtaining information concerning watchlisted individuals." *See* Ex. 4 at 1.

As with the law enforcement privilege invoked by Defendants here, TSA's SSI Final Order likewise makes plain that the fact that these subpoenas are directed at a third party, and while couched in terms of asking that third party to opine on prior statements it made to the media about the purportedly stolen documents, that does not change the underlying SSI concerns. Specifically, the Order concludes:

> In particular, the information sought includes "[c]ommunications with journalists or media outlets about the No Fly List, Selectee List, or any other government watchlist," and "[a]ll details regarding the following statement CommuteAir provided to Daily Dot: 'The server contained data from a 2019 version of the federal no-fly list that included first and last names and dates of birth.' To the extent the information sought would tend to confirm or deny the authenticity of the allegedly leaked data, it constitutes SSI. For example, any testimony or document from CommuteAir that would confirm or deny the accuracy of media statements concerning the alleged data breach constitutes SSI. If the purportedly leaked data is authentic, any official acknowledgement would constitute SSI for all of the same reasons given in Section III.A., *supra*, and would additionally remove lingering and unresolved doubts in the minds of adversaries, which could facilitate the circumvention of security measures. Conversely, if the purportedly leaked data is not authentic, any denial of its authenticity would tend to indicate the authenticity of any other document containing SSI that was purportedly leaked and for which the government has neither confirmed nor denied its authenticity.

Id. at 3-4. Finally, the Order finds that "CommuteAir's statements to the media and information confirming or denying whether such statements were made do not constitute SSI, and are not covered by this SSI Final Order. However, as explained above, information tending to confirm or deny the authenticity of the allegedly leaked data, including any testimony or document that would tend to confirm or deny the *validity of prior media statements*, constitutes SSI for all the reasons discussed in this SSI Final Order." *Id.* (emphasis added).

Finally, Plaintiffs cannot challenge SSI determinations in connection with the instant Motion because, as a final order of TSA, judicial review of SSI orders must occur exclusively

within the Courts of Appeals. *See, e.g.*, *Blitz v. Napolitano*, 700 F.3d 733, 741 (4th Cir. 2012); *Elec. Privacy Info. Ctr. v. Dep't of Homeland Sec.*, 928 F. Supp. 2d 139, 146 (D.D.C. 2013); *Chowdhury v. Northwest Airlines Corp.*, 226 F.R.D. 608, 614 (N.D. Cal. 2004). As the Order itself provides, it was "issued under 49 U.S.C. § 114(r) and is final," and "[p]ursuant to 49 U.S.C. § 46110, any person disclosing a substantial interest in this Order may, within 60 days of its issuance, apply for review by filing a petition for review in an appropriate U.S. Court of Appeals." Ex. 4 at 4. Should Plaintiffs contest this Order, therefore, this court would lack jurisdiction to consider such a challenge, even though the Court would otherwise have jurisdiction to assess the Government's assertion of the law enforcement privilege.

III. In the Alternative, the Court Should Issue a Protective Order Requiring Plaintiffs to Withdraw the Subpoenas.

As an alternative to quashing the subpoenas outright, the Court could also issue a Protective Order that requires Plaintiffs to withdraw the subpoenas. *See Drips Holdings, LLC v. Teledrip LLC*, No. 5:19-CV-02789-JRA, 2021 WL 8342860, at *3 (N.D. Ohio Apr. 15, 2021) ("[T]he Court notes that requiring the withdrawal of a subpoena is also an available remedy under a Rule 26(c) protective order"); *Thogus Prod. Co. v. Bleep, LLC*, No. 1:20CV1887, 2021 WL 827003, at * 5 (N.D. Ohio Mar. 4, 2021) (granting protective order to objecting party requiring withdrawal of subpoenas to nonparties). Here, such a Protective Order could require the Plaintiffs to recraft their subpoenas to protect law enforcement privileged information and SSI, such as by limiting the subpoenas to a request that CommuteAir simply acknowledge that it made the statements to the media that are referenced in the subpoena, without seeking to authenticate the underlying data that was subject to the alleged breach. *See Drips Holdings, LLC v. Teledrip LLC*, 2021 WL 8342860, at *3 ("In other words, a court may issue a protective order that may excuse the third party from appearing to testify or producing documents (which has the same effect as quashing the subpoena)

or it *may impose conditions on when the appearance takes place, what may be asked, or who may read the documents produced in response to the subpoena.*" (citing Fed. R. Civ. P. 26(c)(1)(A)-(H)) (emphasis added). Such a Protective Order would likely ameliorate the Government's concerns about disclosure of SSI and law enforcement privileged information.

IV. At a Minimum, An Emergency Stay Is Warranted.

Given the urgency of the current March 7 deposition date and the contemplated March 4 document production date, the Government at a minimum seeks an emergency stay pending resolution of its Motion to Quash. In evaluating a motion for a stay, courts consider "(1) whether the stay applicant has made a strong showing that he is likely to succeed on the merits; (2) whether the applicant will be irreparably injured absent a stay; (3) whether the issuance of the stay will substantially injure the other parties interested in the proceeding; [and] (4) where the public interest lies." *Hilton v. Braunskill*, 481 U.S. 770, 776 (1987)). Here, the Government believes that it has made a strong showing that it is likely to succeed on its arguments that the subpoenas seek information that is privileged and statutorily protected from disclosure, for similar reasons as those identified by the U.S. District Court for the District of Maryland. Additionally, given that the disclosure of this information itself could cause damage to law enforcement and counterterrorism efforts, the injury to the Government, once any disclosure occurs, could be irreparable.

Perhaps most glaringly, there is simply no injury to Plaintiffs at all in a temporary stay while the parties litigate the privilege issues laid out in this Motion. Plaintiffs have not identified any compelling need for this information *now*, when discovery is ongoing in the underlying lawsuit and the Government has agreed to stipulate that the depositions could go forward at a later date should the Plaintiffs prevail on their arguments. There are no impending deadlines for motions *in limine* or summary judgment briefing in the District of Maryland that would require these

depositions to proceed on March 7. There is therefore no harm at all to Plaintiffs by virtue of a stay; indeed, a stay would be more efficient for the Court and for the parties. *See, e.g., United States v. One Million One Hundred Thirty One Thousand Seven Hundred Ninety Two Dollars in U.S. Currency,* No. 2:17-CV-14005, 2018 WL 11434739, at *1 (E.D. Mich. Oct. 2, 2018) ("Although Claimant could depose the law enforcement officers on issues related only to the undisputed Defendants *in rem*, 'economy of time and effort' for counsel, litigants, and the deposed officers advises otherwise. The Court will therefore stay discovery pending resolution of Plaintiff's motion for an evidentiary hearing, motion for a protective order, and motion to strike.").

Finally, as the U.S. District Court for the District of Maryland again held, "[t]he public interest in nondisclosure is stronger here than the needs of Plaintiffs to have access to the privileged information," *see* Ex. 6 at 25, so there is no argument (compelling or otherwise) that the public interest favors this deposition occurring next week, prior to the Court's assessment of this Motion to Quash. Finally, given the lack of urgency on the part of the Plaintiffs, a stay would give this Court time to consider the important issues raised in this Motion on a more reasonable time frame, with the benefit of full briefing.

CONCLUSION

For the foregoing reasons, Defendants' Emergency Motion for a stay pending further briefing on this Motion should be Granted. In the alternative, the Court should issue a Protective Order requiring the Plaintiffs to withdraw the subpoenas, or should quash the subpoenas altogether.

Dated: February 29, 2024

Respectfully submitted,

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

BRIGHAM J. BOWEN
Assistant Branch Director

/s/Alexander N. Ely

ALEXANDER N. ELY
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street, NW, Washington, DC 20005
Telephone: (202) 993-5177
Facsimile: (202) 616-8470
Alexander.n.ely@usdoj.gov

Counsel for Defendants

CERTIFICATE OF SERVICE

I hereby certify that on February 29, 2024, a copy of the document above was served by email to the following counsel of record for Plaintiffs in the underlying action:

Ahmad Mohamed
CAIR New York
46-01 20th Avenue
Queens, NY 11105
6466657599
Email: ahmedmohamed@cair.com

Gadeir F. Abbas
CAIR
453 New Jersey Ave SE
Washington, DC 20003
202-742-6420
Fax: 202-488-0833
Email: gabbas@cair.com

Justin Mark Sadowsky
Council on American-Islamic Relations
453 New Jersey Avenue
Washington, DC 20003
202-742-6440
Email: jsadowsky@cair.com

Amy V Doukoure
CAIR - Michigan
30201 Orchard Lake Rd. Ste. 260
Farmington Hills, MI 48334
2485592247
Fax: 2485592250
Email: adoukoure@cair.com

Lena F Masri
CAIR
453 New Jersey Ave SE
Washington, DC 20003
202-742-6420
Fax: 202-488-0833
Email: lmasri@cair.com

Hannah Mullen
Council on American-Islamic Relations
453 New Jersey Ave SE
Washington, DC 20003
202-516-4726
Email: hmullen@cair.com

A copy of the document above was also transmitted by email to counsel for third parties CommuteAir and Mr. Erik Kane at the following address:

Peter Turner, Esq.
Partner
Meyers, Roman, Friedberg & Lewis
28601 Chagrin Boulevard, Suite 600
Cleveland, Ohio 44122
p: (216) 831-0042 x162
f: (216) 831-0542
email: pturner@meyersroman.com

/s/ Alexander N. Ely
ALEXANDER N. ELY
Counsel for Defendants